OCEG

DRIVING PRINCIPLED PERFORMANCE®

MOVING ENTERPRISE RISK MANAGEMENT FROM COMPLEXITY TO SIMPLICITY

SPEAKER:

MARSHALL TOBUREN, RSA ARCHER GRC STRATEGIST

marshall.toburen@rsa.com

RSA® Archer GRC

December 5, 2013

OCEG WEBINAR SERIES

Housekeeping

- Download slides at http://www.oceg.org/event/moving-enterprise-risk-management-complexity-simplicity/
- Answer all 3 polls
- Certificates of completion (only for OCEG Premium/Enterprise members and All-Access Pass holders)
- Evaluation survey at the close of the webinar
- Archive at Recorded Events on OCEG site
- Thank you to our webinar sponsor, RSA

Learning Objectives

- Understand the varying pockets of risk information available within your organization
- Develop a common taxonomy or risk "language" across these risk types
- Apply this taxonomy to an overall Risk Management process to identify, assess, decision, treat and monitor risk
- Understand maturity paths to help organizations begin this journey

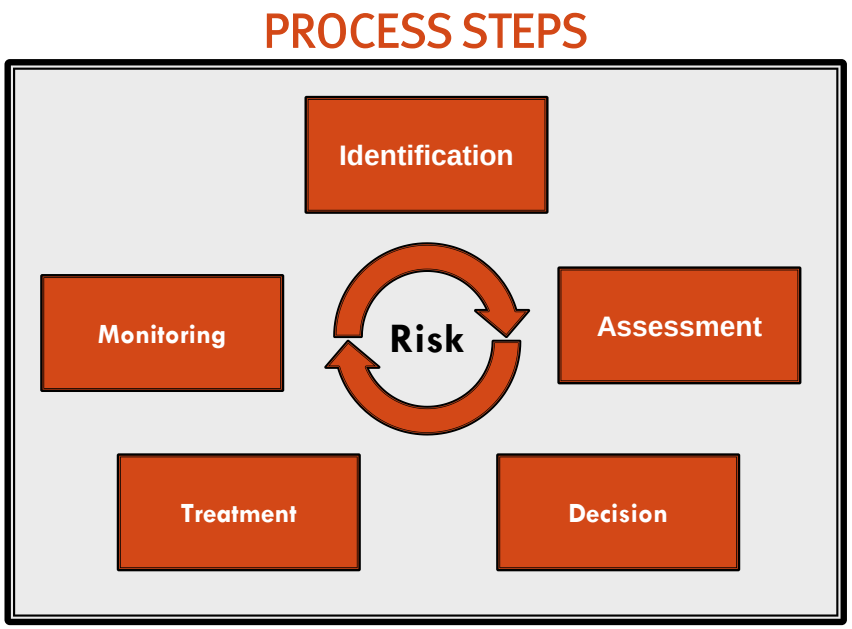
POLL #1

What is the primary driver for your organization's interest in ERM?

A. Avoid / minimize negative risk events
B. Regulatory pressure
C. Performance / strategic optimization
D. It's the latest management craze

Risk Management

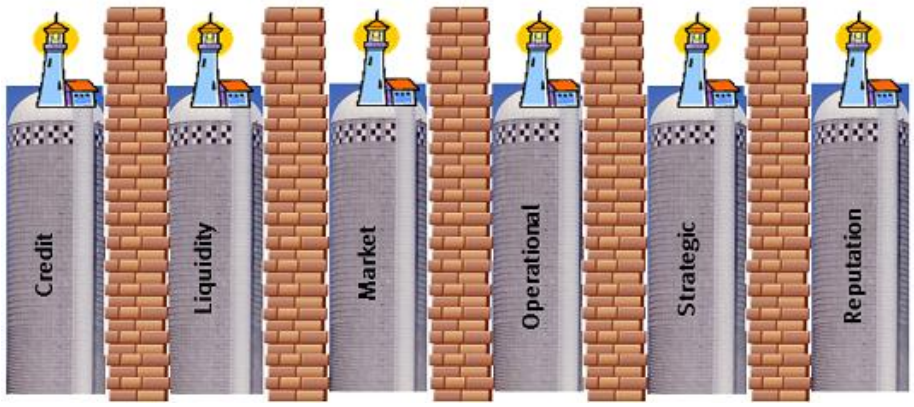
- Core elements of any Risk Management process are risk identification, assessment, decision, treatment, and monitoring
- Organizations build out processes around those framework elements and ERM universe they wish to target
- The breadth of an organization's risk management program will evolve over time depending on the organization's resources, capabilities, and risk management program maturity



- Some characteristics of an ERM program evolve faster than others depending on need, changes in and outside the organization, perceived risk, surprises, and regulatory mandates
- ERM programs achieve maturity through tone at the top, agreed upon terminology, education of stakeholders, iteration, and resources

Incomplete Knowledge of Risks

- No holistic repository of enterprise risks
- Emerging risks from external events
- Acquired risks from mergers & acquisitions
- New ventures (new products, services, markets)
- Changing business process, technologies, & organizational structure
- Changes in institutional knowledge



Inconsistent Risk Assessment

- Unclear or undefined risk taxonomy
- Some areas not performing risk assessments
- Different risk assessment approaches
- Different risk assessment scales
- Risk assessments that don't provide meaningful information

Inconsistent Risk Decision Processes

- Risks without defined, well communicated, or enforced risk appetites and tolerances
- Varying risk tolerances across comparable risks
- Misalignment between different areas of enterprise
- Decisions based on bad information
- Decision processes not adequately formalized
- Changing risk not subject to timely decisions

Suboptimal Risk Treatment

- Uncertain knowledge regarding correct balance of risk treatment vs. risk capacity, appetite, and tolerance
- Risks over-controlled
  - Excessive resource cost
  - Lost opportunities
  - Slow to respond
- Risks under-controlled
  - Surprises
  - Excessive losses

Fragmented & Ineffective Risk Monitoring

- Non-existent monitoring of some activities
- Uncertainty about the key drivers of specific risks and the significance of the drivers
- Poor design (subjective, doesn't capture scenarios)
- Frequency not consistent with risk volatility
- Process prone to error (manual and reliant on SMEs)
- Unaware of changing risk profile
- Inability to predict and avert surprises

Poor Accountability & Risk Culture

- Risk concepts, terms, applicability, & importance not understood by managers
- Risk responsibilities not clearly communicated
- No visible link between manager's risk responsibility and overall risk to organization
- Exceptions & issue escalation without consistent management feedback loop
- Risk taking & compensation not formally linked

Demonstrating ERM Effectiveness & Efficiency

- Satisfying Exec. Mgmt., Board, Auditors & Regulators
- All significant risks captured, assessed correctly, decisioned, treated, & monitored enterprise-wide
- Timely awareness & response to emerging/changing risk
- Understanding where weaknesses in ERM program reside & having active plans to remediate & mature
- No significant surprises

RSA Archer GRC

Management Overhead, Cost, Inefficiency

- Spreadsheet risk management inefficient / prone to error
- Managers bombarded with multiple questionnaires and subject to multiple audit and compliance tests
- Analysts spend too much time on admin tasks
- Knowledge not captured / leveraged for multiple purposes
- Reporting burdensome

OCEG DRIVING PRINCIPLED PERFORMANCE

RSA Archer GRC

Foundational Issues

- Authority
- Scope
- Terminology
  - Risk – both good and bad?
  - Risk Categories
  - Risk Treatment
- Roles and Functions
  - Ownership/accountability of risks, controls, risk-related policies
  - 3 Lines of Defense
  - Key Risk Management Roles
  - Risk Governance Committees

Foundational Issues *(continued)*

- Scope of framework elements
- Approach(es) to risk assessment
  - Risk category classifications
  - Inherent / Residual
  - Likelihood / Impact; Frequency vs. Likelihood
  - Volatility, Threats, Sources
  - Qualitative, Quantitative, Both
  - Business context boundaries
  - Top Down / Bottom Up Assessments / Unification
  - Impact of incentives
  - Existing and Emerging Risk – Workshops, Self-Assessments, Periodic assurance and testing

Foundational Issues *(continued)*

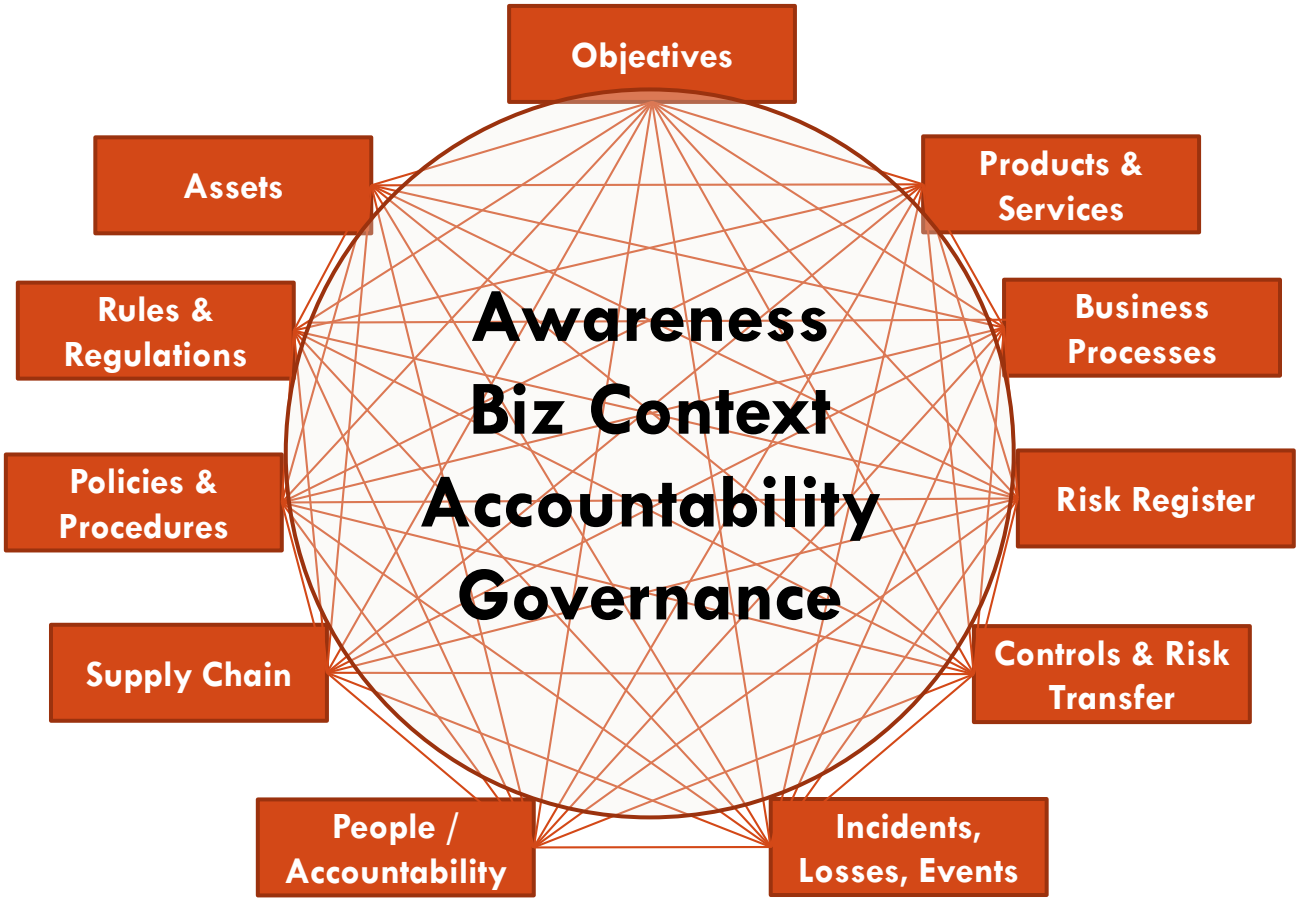
- Rating Scales (Harmonized)
  - Risk Assessment
  - Internal, External, Regulatory Audit Issues
  - Incidents, Events, Losses, Near Misses
  - Visual representation
- Risk Appetite, Tolerance, & Delegated Authorities
  - Decision workflow
  - Exception handling & Escalation
  - Reporting

Foundational Issues *(continued)*

- Communication Structure
  - Management Roll-up
  - Business Hierarchy Roll-Up
  - Financial Roll-up
  - Risk Governance Committee domain
- Information Management
  - Documentation of Efforts
  - ERM Framework Registers
  - Change control
  - Automation tools

ERM Information Architecture

INPUTS
Info from
Systems of Record
KRIs, KCIs, KPIs
Assessments
Assurances
Testing



OUTPUTS
Ownership
Exceptions,
Incidents, Losses
Remediation
Plans
Changes
Decision
Workflow
Dashboards
Notifications
Reports

Operationalizes risk management practices across risk categories; Enables consistent risk decisions; Enables efficiencies across the 3 lines of defense; Fewer surprises; Institutionalizes knowledge; Better decisions; Promotes risk management culture; Provides positive assurance to stakeholders

RSA Archer GRC

POLL #2

What is the status of your ERM system?

A. Risk is managed using silo'd systems and processes and coordinated manually
B. We have a core ERM system and are in the process of integrating inputs from point solutions
C. We have a fully implemented and integrated ERM system
D. I don't know

Phases of Maturity

Phase 1	Phase 2	Phase 3
• Identification of risks limited to auditors & executive management • Risks may not be broadly identified and well documented.	• Risks are assigned to owners • Owners educated about what risk is, its relationship to other framework elements, and how to identify it • A formal risk register exists • Classification of risks by category • ERM framework documentation in process • Primary focus on risks of something going wrong • Root cause analysis of losses & incidents	• Good (strategy & opportunity) & bad risks included in risk identification • ERM framework substantially documented and change control implemented • Defined risk universe is routinely reaffirmed up and down the organization • New & emerging risks regularly solicited & evaluated • Root cause analysis of near misses

RSA Archer GRC

Phases of Maturity

Phase 1	Phase 2	Phase 3
• Ad-hoc assessment of risk • No consistent risk vocabulary • No consistent assessment methodology • No consistent definition of when risks would be considered significant	• Agreed upon risk measurement approach • Standardized risk rating scales used throughout the organization • Substantially qualitative assessments • Some metric based assessments	• Assessment approach consistent enterprise-wide • Significant risk quantified wherever possible using non-subjective metrics • Awareness of interdependent risks • Risks assessments are harmonized • Evaluating actual losses & near misses against expected losses & external data

RSA Archer GRC

Phases of Maturity

Phase 1	Phase 2	Phase 3
• Line managers not explicitly aware of risk ownership • Risk appetite & tolerance not defined • Authority to take risk is not clearly defined and delegated • Risk decisions are ad-hoc and inconsistent • Many risk decisions are heavily influenced by auditors	• Some delegated authorities are formally approved and communicated • Delegated authorities may be inconsistent across processes, risks, risk impacts, and management levels • Process of escalating and documenting risk decisions not handled consistently	• Risk appetite & tolerance formally and consistently defined for all major risk categories • Managers understand their risk taking authority • Systems enforce authorities where appropriate • Systems escalate exceptions to managers with appropriate authority & decisions formally documented

Phases of Maturity

Phase 1	Phase 2	Phase 3
• Internal controls may be documented by auditors • The relationship between controls and the risks they mitigate may not be clear	• Controls are assigned to owners • Owners are educated about controls, why they are important, and how to identify and describe them • A formal control register exists that is linked to risks, policies, & regs. • Owners periodically attest to the operation of controls • Control design and effectiveness assessments and tests are captured	• Consideration of all risk treatment types, not just controls (insurance and hedging) • Remediation plans to bring risks and risk drivers within tolerances are formalized and actively managed • Total cost of risk is considered, where significant and risk treatment adjusted when not justified

Phases of Maturity

Phase 1	Phase 2	Phase 3
• Limited use of metrics • Reporting is burdensome and mostly manually compiled • Some risk reporting is ad-hoc and focused on the risk du jour • Risk & control gap reports are not available or easily compiled • No central repository of remediation plans	• Some metrics (primarily loss monitoring) used within the organization • Risk and control register reporting exists that may roll-up into summary and executive level reports • Gaps, outstanding issues, and remediation plans are centrally compiled and monitored	• Metrics widely implemented and monitored around significant ERM framework elements • Robust, actionable, reporting is in place at all levels of the organization • ERM framework elements that deviate from specified tolerances are automatically reported to key stakeholders • Gaps & issues not remediated within agreed upon timeframes are automatically escalated

Phases of Maturity

Phase 1	Phase 2	Phase 3
• BOD & C-Suite acknowledge risk management importance • Some risk categories are subject to on-going oversight, mostly where problems have cropped up or regulatory pressures • Risks are managed inconsistently within silos • Risk taxonomy specific to risks being managed • Oversight rolls-up to different areas within the organization • Reactive risk management	• Top-down commitment to RM communicated across enterprise • Code of conduct • Accountability for all risk assigned to chief risk officer • Holistic risk taxonomy created and communicated throughout the organization • Roles & responsibilities documented - 3 Lines of Defense Enabled • Governance integration	• Delegated authorities communicated consistent with appetite and tolerance • Culture developed where everyone is a risk manager • Transparency into all significant risk categories through one unified view • Proactive risk management • ERM aligned with performance optimization & strategy

Additional Resources from RSA Archer

- Marshall Toburen, GRC Strategist
  marshall.toburen@rsa.com
- RSA Archer private Community and Exchange
- RSA Public web site: http://www.emc.com/security/rsa-archer.htm
- Weekly complementary webcasts on various GRC leadership topics http://www.emc.com/campaign/global/rsa/rsa-webcast.htm
- GRC leadership blogs from myself and my colleagues https://community.emc.com/community/connect/grc_ecosystem

POLL #3

Are you a PAID member of OCEG who is interested in receiving CPE credit for this event?

A. Yes, I am a PAID OCEG member and would like to receive a Certificate of Completion for this event

B. No, I am not a PAID OCEG member

Questions?